

DATASHEET

ManageEngine[®]
ADAudit Plus

Un audit des changements basé sur l'UBA

Protégez votre entreprise contre les menaces internes et les cyberattaques en auditant votre Active Directory (AD), vos serveurs de fichiers, vos serveurs Windows et vos postes de travail avec ManageEngine ADAudit Plus.



Audit des changements dans l'Active Directory et Azure AD

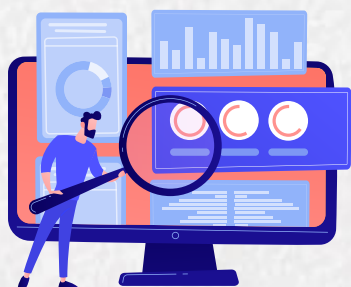
- » **Audit des changements AD :**
Suivez les modifications apportées aux unités d'organisation (OU), utilisateurs, groupes, ordinateurs, groupes administratifs et autres objets AD.
- » **Suivi des modifications d'autorisations AD**
Affichez toutes les modifications des autorisations AD, telles que celles apportées aux autorisations au niveau domaine, aux OU, au schéma, à la configuration et au DNS.
- » **Tracer l'historique des changements d'objets :**
Recevez des rapports d'audit détaillés sur les modifications avec des informations sur les anciennes et nouvelles valeurs des attributs modifiés.
- » **Audit de la gestion des comptes utilisateurs :**
Suivez la création, la suppression et la modification des utilisateurs, la réinitialisation des mots de passe et les autres actions de gestion des comptes.
- » **Surveiller les changements DNS et de schémas :**
Obtenez une visibilité sur l'ajout, la modification et la suppression des nœuds et des zones DNS, surveillez les changements de schéma et de configuration AD.
- » **Surveillance des environnements AD hybrides :**
Obtenez une vue unifiée de toutes les activités se déroulant dans vos environnements AD on-premises et Azure, avec des alertes pour les événements critiques.

Modules de licence :

Contrôleurs de domaine, Tenants
Azure AD

Plateformes prises en charge :

Windows Server 2003 et supérieur



Surveillance des modifications de fichiers

- » **Surveiller les accès aux fichiers et aux dossiers :**
 Suivez en temps réel les tentatives d'accès aux fichiers, qu'elles soient réussies ou non (création, lecture, suppression, modification, copier-coller, transfert)..
- » **Rapport sur les modifications apportées aux fichiers partagés :**
 Suivez chaque accès et chaque modification apportée aux fichiers et dossiers partagés dans votre domaine, avec des détails sur qui a accédé à quoi, quand et à partir d'où.
- » **Audit des changements d'autorisation :**
 Suivez les changements d'autorisation NTFS et de partage avec des détails tels que leurs anciennes et nouvelles valeurs.
- » **Simplifier les audits de conformité :**
 Recevez des rapports prêts à l'emploi pour HIPAA, RGPD, FISMA, PCI DSS, SOX, GLBA, ISO 27001.
- » **Contrôler l'intégrité des fichiers :**
 Recevez des rapports détaillés sur toutes les modifications apportées aux fichiers système et programme critiques, et déclenchez des alertes lorsqu'une activité suspecte est détectée.
- » **Audit sur plusieurs plateformes :**
 Visualisez les modifications apportées aux serveurs de fichiers Windows, clusters de basculement, filers NetApp, NAS Synology, NAS Hitachi, EMC VNX, VNXe, Isilon, Celerra et Unity à partir d'une seule console.

Modules de licence :
 Contrôleurs de domaine

Plateformes prises en charge :

Windows Server 2003 et supérieur • Dell VNX, VNXe, Celerra, Unity, et Isilon • Synology DSM 5.0 et supérieur
 • NetApp ONTAP 7.2 et versions supérieures pour les filers • NetApp ONTAP 8.2.1 et versions supérieures pour les clusters • Hitachi NAS 13.2 et versions supérieures • Systèmes de stockage Huawei OceanStor V5 series et OceanStor 9000 V5.



Audit des changements des paramètres de stratégie de groupe

- » **Audit des objets de stratégie de groupe :**
Gardez un œil sur la création, la suppression et la modification des objets de stratégie de groupe (GPO).
- » **Suivi des modifications des paramètres GPO :**
.Suivez les modifications apportées aux paramètres GPO et voyez qui a modifié quel paramètre, quand, à partir d'où, et les valeurs du paramètre avant et après la modification.
- » **Tracer l'historique des changements de GPO :**
Visualisez l'historique des modifications d'une ou de plusieurs GPO dans un domaine afin de détecter les activités injustifiées.
- » **Configurer des alertes pour les changements critiques :**
Déclenchez des alertes instantanées par e-mail et SMS pour les changements critiques, tels que les changements de configuration ordinateur et les changements de stratégie de verrouillage des mots de passe et des comptes.
- » **Planifier des rapports sur les changements de GPO :**
Envoyez des rapports planifiés sur les modifications importantes des GPO ou des paramètres de GPO à des destinataires spécifiques.

Modules de licence :
Contrôleurs de domaine

Plateformes prises en charge :
Windows Server 2003 et supérieur



Audit et rapports des serveurs Windows

» Auditer les serveurs Windows :

Surveillez les modifications apportées aux membres des groupes administratifs locaux, aux utilisateurs locaux, aux droits des utilisateurs, aux stratégies locales.

» Suivi des tâches et processus planifiés :

Créez des rapports sur la création, la suppression et la modification des tâches et processus planifiés.

» Surveiller l'utilisation des USB et des imprimantes :

Suivez l'utilisation de l'USB et les transferts de fichiers vers des périphériques de stockage amovibles. Suivez également quel fichier a été imprimé, quand, par qui, le nombre de pages et de copies imprimées.

» Audit des processus PowerShell :

Surveillez les processus PowerShell qui s'exécutent sur vos serveurs Windows, ainsi que les commandes qui y sont exécutées.

» Surveiller l'ADFS, LAPS et ADLDS :

Suivez les tentatives d'authentification ADFS, les utilisateurs qui ont consulté les mots de passe des administrateurs locaux, les modifications apportées à l'heure ou à la date d'expiration d'un mot de passe.

Modules de licence :

Serveurs membres

Plateformes prises en charge :

Windows Server 2003 et supérieur



Audit des ouvertures et fermetures de session

» Auditer les ouvertures et fermetures de session :

Suivez l'activité de connexion et de déconnexion ainsi que la durée de connexion sur vos contrôleurs de domaine (DC), serveurs Windows et postes de travail.

» Suivre l'historique des connexions utilisateurs :

Enregistrez l'activité de connexion de chaque utilisateur, identifiez les utilisateurs qui sont actuellement connectés, répertoriez les utilisateurs connectés à plusieurs machines,...

» Audit des connexions RADIUS :

Obtenez une visibilité sur les connexions à vos serveurs RADIUS grâce à des rapports sur les connexions RADIUS, les échecs de connexion et l'historique des connexions RADIUS (NPS).

» Analyser les échecs de connexion :

Suivez toutes les tentatives d'ouverture de session qui ont échoué en indiquant qui a tenté de se connecter, sur quelle machine, à quel moment et la raison de l'échec.

» Répondre aux activités de connexion malveillantes :

Tirez parti de l'apprentissage machine pour repérer et répondre rapidement à des volumes inhabituels d'échecs de connexion, à des durées de connexion inhabituelles.

Modules de licence :

Contrôleurs de domaine, Serveurs membres, Postes de travail.

Plateformes prises en charge :

• Windows Server 2003 et supérieur • Windows XP et supérieur



Analyse de verrouillage des comptes

- » **Recevoir des notifications de verrouillage de comptes :**
 Détectez les verrouillages de comptes utilisateurs AD en temps réel grâce à des alertes par e-mail et SMS, et réduisez la durée de verrouillage des comptes.
- » **Examiner les verrouillages de comptes avec l'UBA :**
 Identifiez les utilisateurs négligents et les personnes internes malveillantes en repérant les activités de verrouillage anormales grâce à l'analyse du comportement des utilisateurs (UBA).
- » **Trouver la source de verrouillage du compte :**
 Analysez les connexions par téléphone portable, les sessions RDP, les services, les tâches planifiées pour détecter les informations d'identification obsolètes et identifier la source des verrouillages de comptes.
- » **Améliorer l'efficacité du helpdesk :**
 Affichez des rapports contenant toutes les informations nécessaires au personnel du helpdesk pour résoudre plus rapidement les problèmes de verrouillage du compte et minimiser les temps d'arrêt du service..
- » **Vérifier l'état de verrouillage des comptes :**
 Obtenez des rapports sur l'état de chaque compte verrouillé, l'heure à laquelle le verrouillage s'est produit.
- » **Analyser la cause profonde :**
 Conserver une liste d'audit claire des réinitialisations de mot de passe, des modifications de mot de passe et des sources de verrouillage de compte afin de simplifier l'analyse forensique.

License modules:

Domain Controllers, Member Servers, Workstations

Supported platforms:

• Windows Server 2003 and above • Windows XP and above



Suivi de l'activité des employés

- » **Mesurer la productivité des employés :**
Découvrez comment les employés passent leurs heures de travail grâce aux heures de démarrage et d'arrêt de l'ordinateur, aux détails de l'historique des connexions, à l'activité des fichiers.
- » **Suivi de la présence des employés :**
Tenez des feuilles de temps précises pour vos employés avec leurs heures d'arrivée et de départ, et analysez la durée de leur connexion.
- » **Calculer les heures de travail réelles :**
Trouvez la liste des utilisateurs actuellement connectés et calculez leurs heures de travail réelles avec des détails sur les moments où ils étaient actifs et inactifs.
- » **Surveiller les travailleurs à distance :**
Suivez les ouvertures de session par la passerelle de bureau à distance et RADIUS, et découvrez qui a tenté de se connecter à distance, à quel moment, s'il a réussi et combien de temps a duré sa session.
- » **Surveiller l'activité informatique des employés :**
Trouvez les heures de démarrage et d'arrêt récentes d'un ordinateur, ainsi que des détails sur l'auteur, le type d'arrêt.
- » **Identifier les activités de connexion à risque :**
Repérez et analysez les tentatives répétées et infructueuses de connexion à des postes de travail, des machines distantes et des serveurs critiques grâce à des alertes instantanées par e-mail et SMS.

Modules de licence : Postes de travail

Plateformes prises en charge :
Windows XP et supérieur



Surveillance des utilisateurs privilégiés

- » **Auditer l'activité des administrateurs :**
Suivez les actions des administrateurs sur le schéma AD, la configuration, les utilisateurs, les groupes, les OU, les GPO.
- » **Repérer les anomalies comportementales :**
Identifiez les actions qui s'écartent des modèles d'accès normaux pour trouver les pirates qui utilisent des informations d'identification volées ou partagées de comptes privilégiés.
- » **Examiner l'activité des utilisateurs privilégiés :**
Respectez les différentes réglementations informatiques en conservant une liste d'audit des activités effectuées par les utilisateurs privilégiés dans votre domaine.
- » **Recevoir des alertes sur les activités suspectes :**
Repérez et répondez rapidement aux événements à haut risque, tels que l'effacement des logs d'audit ou l'accès à des données critiques en dehors des heures de bureau, grâce à des alertes instantanées.
- » **Détecter l'élévation de privilèges :**
Identifiez l'élévation de privilèges grâce à des rapports documentant la première utilisation des privilèges par les utilisateurs, et vérifiez si les privilèges d'un utilisateur sont nécessaires pour son rôle.

Modules de licence :

Contrôleurs de domaine, Serveurs membres

Plateformes prises en charge :

Windows Server 2003 et supérieur



Détection des malwares et des menaces internes

- » **Recherche de menaces alimentée par l'UBA :**
 Détectez rapidement les échecs de connexion répétés, les anomalies dans l'activité des utilisateurs, les élévations de privilèges, l'exfiltration de données grâce à l'UBA.
- » **Détecter les intrusions de ransomware :**
 Repérez les indicateurs révélateurs d'intrusions de ransomware tels que les pics inhabituels de renommage, de suppression ou de changement d'autorisation de fichiers.
- » **Répondre instantanément aux menaces :**
 Exécutez automatiquement des scripts pour arrêter des machines, des sessions d'utilisateurs finaux, ou effectuez d'autres réponses sur mesure pour atténuer les menaces.
- » **Identifier les anomalies dans l'activité des fichiers :**
 Déclenchez des alertes en cas d'activités suspectes telles que la suppression de fichiers critiques, des accès soudains aux fichiers ou des activités de fichiers à des heures inhabituelles.
- » **Détecter les mouvements latéraux :**
 Repérez les indicateurs de mouvements latéraux tels que des activités de bureau à distance inhabituelles ou l'exécution de nouveaux processus.

Modules de licence :

Contrôleurs de domaine, Serveurs membres, Serveurs de fichiers Windows, Serveurs NAS, Postes de travail.

Plateformes prises en charge :

Windows Server 2003 et supérieur • Dell VNX, VNXe, Celerra, Unity et Isilon • Synology DSM 5.0 et supérieur
 • NetApp ONTAP 7.2 et versions supérieures pour les filers • NetApp ONTAP 8.2.1 et versions supérieures pour les clusters • Hitachi NAS 13.2 et versions supérieures • Systèmes de stockage Huawei OceanStor V5 series et OceanStor 9000 V5 • Windows XP et supérieur



Rapports de conformité

» Exploiter plus de 250 rapports :

Réalisez facilement des audits de conformité grâce à des rapports détaillés sur les modifications apportées à l'AD, aux serveurs de fichiers, aux serveurs Windows et aux postes de travail.

» Recevoir des rapports d'audit prêts à l'emploi :

Planifiez des rapports périodiques prêts à l'emploi pour HIPAA, PCI DSS, RGPD, ISO 27001, GLBA, FISMA et SOX, et personnalisez les rapports pour d'autres réglementations.

» Effectuer une analyse des causes profondes :

En cas de violation, analysez l'incident en profondeur, identifiez la source des fuites ou des intrusions à l'aide de données forensiques précises et partagez vos conclusions avec des rapports personnalisés.

» Contrôler l'intégrité des fichiers :

Suivez tous les accès aux fichiers du système d'exploitation, des bases de données et des logiciels, aux journaux et rapports d'audit archivés et aux autres fichiers critiques.

» Configurer des alertes instantanées :

Détectez rapidement les incidents de sécurité à l'aide d'alertes par e-mail et SMS spécifiques aux fichiers, utilisateurs, périodes de temps ou événements. Réduisez les faux positifs grâce à l'UBA.

» Limiter les dégâts avec des réponses automatisées :

Gagnez un temps précieux avec des réponses automatisées, comme l'exécution de scripts personnalisés pour désactiver des comptes ou arrêter des appareils.

Modules de licence :

Contrôleurs de domaine, Serveurs membres, Serveurs de fichiers Windows, Serveurs NAS, Postes de travail.

Plateformes prises en charge :

Windows Server 2003 et supérieur • Dell VNX, VNXe, Celerra, Unity, et Isilon • Synology DSM 5.0 et supérieur • NetApp ONTAP 7.2 et versions supérieures pour les filers • NetApp ONTAP 8.2.1 et versions supérieures pour les clusters • Hitachi NAS 13.2 et versions supérieures • Systèmes de stockage Huawei OceanStor V5 series et OceanStor 9000 V5 • Windows XP et supérieur

Configuration requise

Pour connaître la configuration requise complète, consultez le [Guide de démarrage rapide](#).

Navigateurs supportés :

Internet Explorer 8 et supérieur, Mozilla Firefox 3.6 et supérieur, Google Chrome, Microsoft Edge

Processeur : 2.4GHz

RAM : 8GB

Espace de disque : 50GB

Plateformes supportées

Audit des DC et serveurs membres	Audit des fichiers	Autres composants
<p>Versions Windows Server :</p> <p>2003/2003 R2 2008/2008 R2 2012/2012 R2 2016/2016 R2 2019</p>	<p>Audit des serveurs de fichiers Windows :</p> <p>Windows File Server 2003 et supérieur</p> <p>Audit EMC :</p> <p>VNX, VNXe, Celerra, Unity, Isilon</p> <p>Audit Synology :</p> <p>DSM 5.0 et supérieur</p> <p>Audit des filers NetApp :</p> <p>Data ONTAP 7.2 et supérieur</p> <p>Audit des clusters NetApp :</p> <p>Data ONTAP 8.2.1 et supérieur</p> <p>Audit NAS Hitachi :</p> <p>Hitachi NAS 13.2 et supérieur</p> <p>Audit Huawei OceanStor :</p> <p>OceanStor V5 series et OceanStor 9000 V5</p>	<p>Audit ADFS :</p> <p>ADFS 2.0 et supérieur</p> <p>Audit des postes de travail :</p> <p>Windows XP et supérieur</p> <p>Audit PowerShell :</p> <p>PowerShell 4.0 ou 5.0</p>

Éditions disponibles



ÉDITION GRATUITE

N'expire jamais

Audit et collecte de données sur 25 postes de travail

Génère des rapports à partir des données de journal collectées pendant l'évaluation

[Essayez maintenant](#)



ÉDITION STANDARD

Toutes les fonctionnalités de l'édition gratuite

+

Rapports et alertes sur les données de journal des événements collectées à partir de ces composants sous licence :

- ✓ Tenants Azure AD
- ✓ Serveurs Windows
- ✓ Postes de travail
- ✓ Serveurs de fichiers
- ✓ Windows
- ✓ Périphériques NAS

[Essayez maintenant](#)



ÉDITION PROFESSIONNELLE

Analyse du verrouillage des comptes

Audit des changements d'autorisation AD

Audit des changements de paramètres des GPO

Audit des changements DNS et schéma AD

Changements d'anciennes et de nouvelles valeurs d'attributs d'objets AD

Prise en charge des bases de données MS SQL

Et bien d'autres choses encore

[Essayez maintenant](#)

PG Software

ManageEngine ADAudit Plus

Un audit des changements basé sur l'UBA qui assure la sécurité et la conformité de votre AD, de vos serveurs Windows, serveurs de fichiers et postes de travail.

Télécharger maintenant

Gratuit, essai de 30 jours

Détails du contact

Site web :

<https://www.pgsoftware.fr>

Obtenir un devis :

<https://www.pgsoftware.fr/iam/adaudit-plus/cotation.html>

Démo en ligne :

<https://www.pgsoftware.fr/contact>

E-mail support technique :

helpdesk@pgsoftware.support

Renseignements commerciaux :

commercial@pgsoftware.fr

Appel Gratuit :

0 805 296 540 Service & appel gratuits